CYBERSECURITY

SCANNING: SCANME.NMAP.COM

SCANME ADVANCED

The Nmap company has provided an online machine to scan: scname.nmap.com (Detected in a previous lab.)

Perform the following tasks:

In this section, we will scan TCP ports in several different ways to gather information on an example target system. We will not scan UDP ports, as we do not have enough time in lab to wait for the 15-20 minutes a UDP scan can take.

3.1 What ports are open on the scanme.nmap.org test server? Use a TCP connect scan. Your answer must include only the port numbers. Do not include other parts of nmap output.

3.2: Using a TCP SYN scan, what ports do you find open on scanme.nmap.org?

3.3: Looking at the output of the two scans outside the ports listed, what differences do you find between the TCP connect and SYN scans? If there is no difference, then just write "None" below.

3.4: Some machines are behind a firewall, which filters connections to some ports, preventing nmap from receiving any response from those ports. Blocked ports may be listed as either "filtered" or "closed". To see an example of such a scan, perform a TCP connect scan on `www.example.com`. Your answer must include port numbers for both closed and open ports. Do not include other parts of nmap output.
Letop: www.example.com geeft enkel open poorten terug. De kern van de vraag is: hoe vind ik alle poorten die nmap gescand heeft, dus ook de "filtered" ports.

3.5: To determine why a scan returns the results that it does, use the `--reason` option. Explain the reasons that ports are listed as open, closed, or filtered in the scan of `scanme.nmap.org`.

3.6: To see every packet sent by a scan, use the `--packet-trace` option. We will save this output in a file for further analysis using I/O redirection. We do not redirect STDERR, so we will still see error output on the screen.

In the box below, explain what packet is sent first in the scan and count how many packets are sent in total. Use a command to do the counting for you, but be sure not to count regular nmap output (what you would see without the trace option).

3.7: The `nmap` scanner can return additional information, including service versions, OS identification, and tracerouting. The `-A` option will perform all of these tests. The `-T4` option tells nmap to use aggressive packet timing, which can be dangerous as it can cause some older machines to crash. However, `scanme.nmap.org` is configured so that it will have no problems with the `-T4` option. Even with the faster speed, this scan will take longer than previous ones due to the large number of tests performed. We add the `-v` option so that you can see the scan in progress

Based on the output of the scan above, answer the following questions:

1. What is the server software name and version for each of the ports?
2. What title would you see in the top of your web browser if you contacted the web server at scanme.nmap.org?
3. How many network hops does it take to reach scanme.nmap.org from your VM?

1. 2. 3.

3.8: By default, nmap scans the most common 1000 ports. With the fast option, nmap scans only 100 ports. Using the -p option, we can configure nmap to configure specific sets of ports, ranging from 1 port to the entire 65,536 possible ports. Scanning all ports can take around 10 minutes over the Internet, so we will scan a local server for this question. How many open ports did you find for each of the scans? How many wall clock (real) seconds did it take for each port scan to finish?

3.9: UDP scans are much slower than TCP scans due to the unreliability of UDP, so the scan in this question will require the longest amount of time. Write the list of open UDP ports in the box below.